

CLAIMS

What is claimed is:

- Sub
A2
- 006030-269960
- 1 1. A method of securely communicating information in a network that includes a host
2 that originates a request, a first server that serves a response to the request, and a
3 second server that cooperates with the first server to respond to the request, the
4 method comprising the computer-implemented steps of:
5 receiving a first request for a service from the host, which request includes a network
6 address of the host; and
7 communicating a second service request to the second server based on the first service
8 request and including the host network address only when a first network
9 address of the first server is identical to a second network address of the
10 second server.
 - 1 2. A method as recited in Claim 1, wherein the request of the host comprises a key value
2 comprising an originating host Internet Protocol (IP) address and a random value.
 - 1 3. A method as recited in Claim 1, wherein the step of communicating a second service
2 request comprises the step of accepting the host request only when an IP address of
3 the second server is the same as an IP address of the first server.
 - 1 4. A method as recited in Claim 1, wherein the host is a Web browser and wherein the
2 host request comprises a Universal Resource Locator (URL) that includes an IP
3 address of the host.
 - 1 5. A method as recited in Claim 1, wherein the host is a Web browser and wherein the
2 host request comprises an HTML POST form that includes an IP address of the host.
 - 1 6. A method of securely communicating data between a proxy server and a second
2 server, wherein each of the proxy server and the second server are addressable by first

3 and second Internet Protocol (IP) addresses, respectively, the method comprising the
4 computer-implemented steps of:

5 receiving, at the proxy server, a first service request from a browser client, wherein the
6 service request includes a third IP address of a client computer associated with
7 the browser client;

8 communicating a second service request that includes the browser client IP address to
9 the second server only when the first IP address of the proxy server is identical
10 to the second IP address of the second server.

1 7. A method as recited in Claim 6, wherein the first service request of the browser client
2 comprises a key value comprising the third IP address and a random value.

1 8. A method as recited in Claim 6, wherein the first service request of the browser client
2 comprises a Universal Resource Locator (URL) that includes an IP address of the
3 host.

1 9. A method as recited in Claim 6, wherein the first service request of the browser client
2 comprises an HTML POST form that includes an IP address of the host.

1 10. A method of securely communicating a network address of a client that issues service
2 requests to a first server that proxies the service requests for a second server,
3 comprising the computer-implemented steps of:
4 receiving a network address of the client;
5 determining whether a first network address of the first server is equal to a second
6 network address of the second server; and
7 sending the network address of the client from the first server to the second server in a
8 secure request message only when the first network address of the first server
9 is equal to the second network address of the second server.

- 1 11. A method as recited in Claim 10, wherein each of the service requests of the browser
2 client comprises a key value comprising an IP address of the client and a random
3 value.
- 1 12. A method as recited in Claim 10, wherein each of the service requests of the browser
2 client comprises a Universal Resource Locator (URL) that includes an IP address of
3 the browser client.
- 1 13. A method as recited in Claim 10, wherein each of the service requests of the browser
2 client comprises an HTML POST form that includes an IP address of the browser
3 client.
- 1 14. A data communications apparatus that securely communicates a service request that is
2 received from a client, comprising a first server that proxies the service request for a
3 second server, the first server comprising means for receiving a network address of the
4 client; means for determining whether a first network address of the first server is
5 equal to a second network address of the second server; and means for sending the
6 network address of the client from the first server to the second server in a secure
7 request message only when the first network address of the first server is equal to the
8 second network address of the second server.
- 1 15. An apparatus as recited in Claim 14, wherein the service request comprises a key
2 value comprising an IP address of the client and a random value.
- 1 16. An apparatus as recited in Claim 14, wherein the service request comprises a
2 Universal Resource Locator (URL) that includes an IP address of the browser client.

- 1 17. An apparatus as recited in Claim 14, wherein the service request comprises an HTML
2 POST form that includes an IP address of the browser client.
- 1 18. A computer-readable medium carrying one or more sequences of instructions for
2 securely communicating a network address of a client that issues service requests to a
3 first server that proxies the service requests for a second server, wherein execution of
4 the one or more sequences of instructions by one or more processors causes the one or
5 more processors to perform the steps of:
6 receiving a network address of the client;
7 determining whether a first network address of the first server is equal to a second
8 network address of the second server; and
9 sending the network address of the client from the first server to the second server in a
10 secure request message only when the first network address of the first server
11 is equal to the second network address of the second server.
- 1 19. A computer-readable medium as recited in Claim 18, wherein each of the service
2 requests of the browser client comprises a key value comprising an IP address of the
3 client and a random value.
- 1 20. A computer-readable medium as recited in Claim 18, wherein each of the service
2 requests of the browser client comprises a Universal Resource Locator (URL) that
3 includes an IP address of the browser client.
- 1 21. A computer-readable medium as recited in Claim 18, wherein each of the service
2 requests of the browser client comprises an HTML POST form that includes an IP
3 address of the browser client.

- 1 22. A data communications apparatus that securely communicates a service request that is
2 received from a client, comprising:
3 a first server that proxies the service request for a second server comprising a network
4 interface to a network that includes the first server and the second server;
5 a processor in the first server;
6 a storage device in the first server comprising one or more sequences of stored
7 instructions which, when executed by the processor, cause the processor to
8 carry out the steps of
9 receiving a network address of the client;
10 determining whether a first network address of the first server is equal to a
11 second network address of the second server; and
12 sending the network address of the client from the first server to the second
13 server in a secure request message only when the first network address of the
14 first server is equal to the second network address of the second server.
- 1 23. An apparatus as recited in Claim 22, wherein the service request comprises a key
2 value comprising an IP address of the client and a random value.
- 1 24. An apparatus as recited in Claim 22, wherein the service request comprises a
2 Universal Resource Locator (URL) that includes an IP address of the browser client.
- 1 25. An apparatus as recited in Claim 22, wherein the service request comprises an HTML
2 POST form that includes an IP address of the browser client.